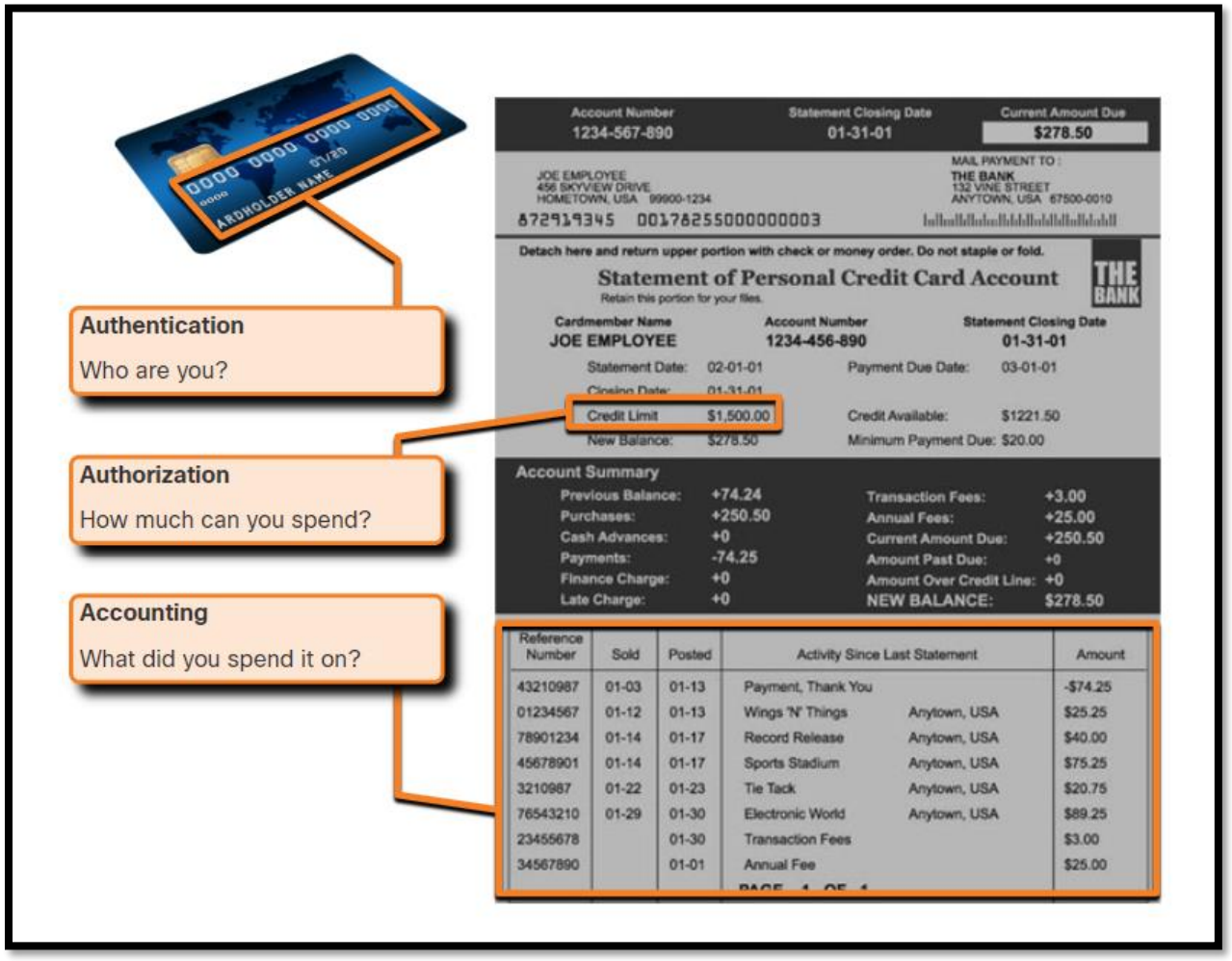

Networkforyou
Welcome
To
Network for you
AAA
Networkforyou

AAA:



AAA (Authentication, Authorization and Accounting):

- Authentication: Verify the identity of the user, who are you.
- Authorization: What is the user allowed to do? Example what resource he can access etc? (How much you can spend)
- Accounting: It is like all record what is done by that user it will keep all record. Example used for billing and auditing (What did you spend it on record)

AAA Stand for Authentication, Authorization and Accounting:

- It is a Centralized Management of users to access the network devices

- AAA Server allow setting up access control on Cisco Routers and Switches
- Like if we have 300 Switches and 10 Router in our organization then it will be very difficult to create all user in that all devices and delete when they leave organization etc. And it will take lot of memory of devise also to overcome with this type of issues we use AAA Server.
- AAA Server also control connections passing through router or switch for access network.
- When every user tries to connect to router or switch these network devices verifies by AAA Server (AAA Database)
- User Management is done with AAA Server without need to reconfigure to individual router or switch
- Like any new user came we need to configure only in AAA Server no need to add that user in Router or switch.
- AAA Server use two Main type of Protocol to configure this
- Radius Protocol (Remote Authentication Dial-in User Service)
- TACACS+ (Terminal Access Controller Access-Control System Plus)

Radius Protocol:

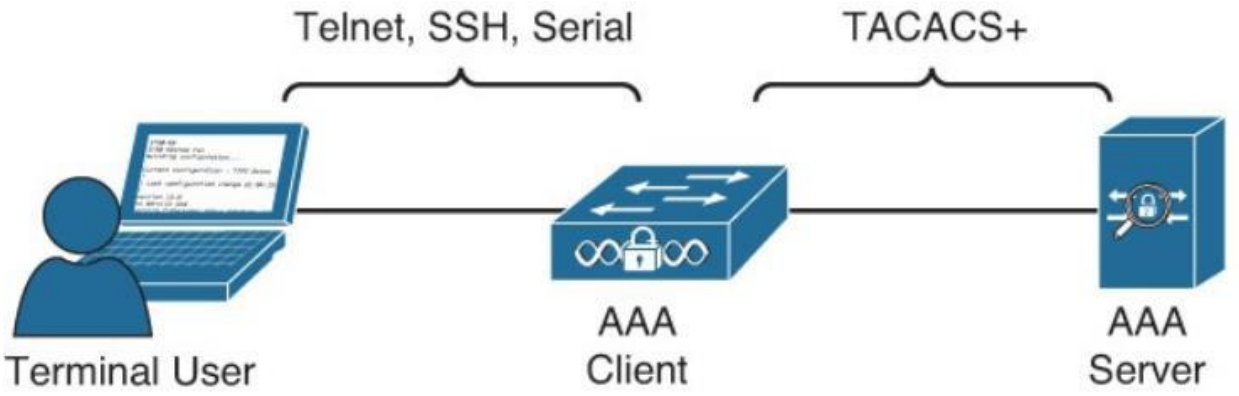
- It is open standard where as TACACS is Cisco Proprietary protocol.
- It uses UDP and users ports numbers 1812/1645 and 1813/1646.
- It Encrypts passwords only.
- It is light weight protocol (Consume less resources).

TACACS+:

- It is CISCO Proprietary protocol.
- It use TCP and port number user 49.
- It encrypts entire communication.
- It is heavy weight protocol consuming more resources.

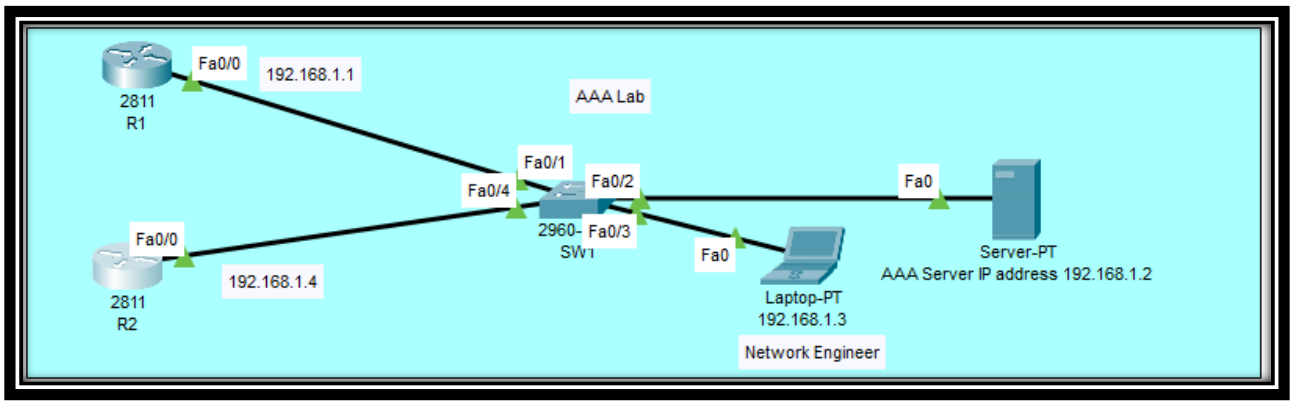
Device Administration:

- Controlling access to who can log in to a network device console, telnet, SSH session.
- Controlling access to who can log in to a network device via other methods.
- Device administration is a process of AAA for controlling the access to network device.
- With any methods via Telnet session, VTY, TTY, SSH session or via Console.
- Device Administrator is user logs into the network devices such as switches routers etc.
- In order to perform the configuration and maintenance of the administered devices.
- There are two uses of AAA, Device Administration and Network Access.



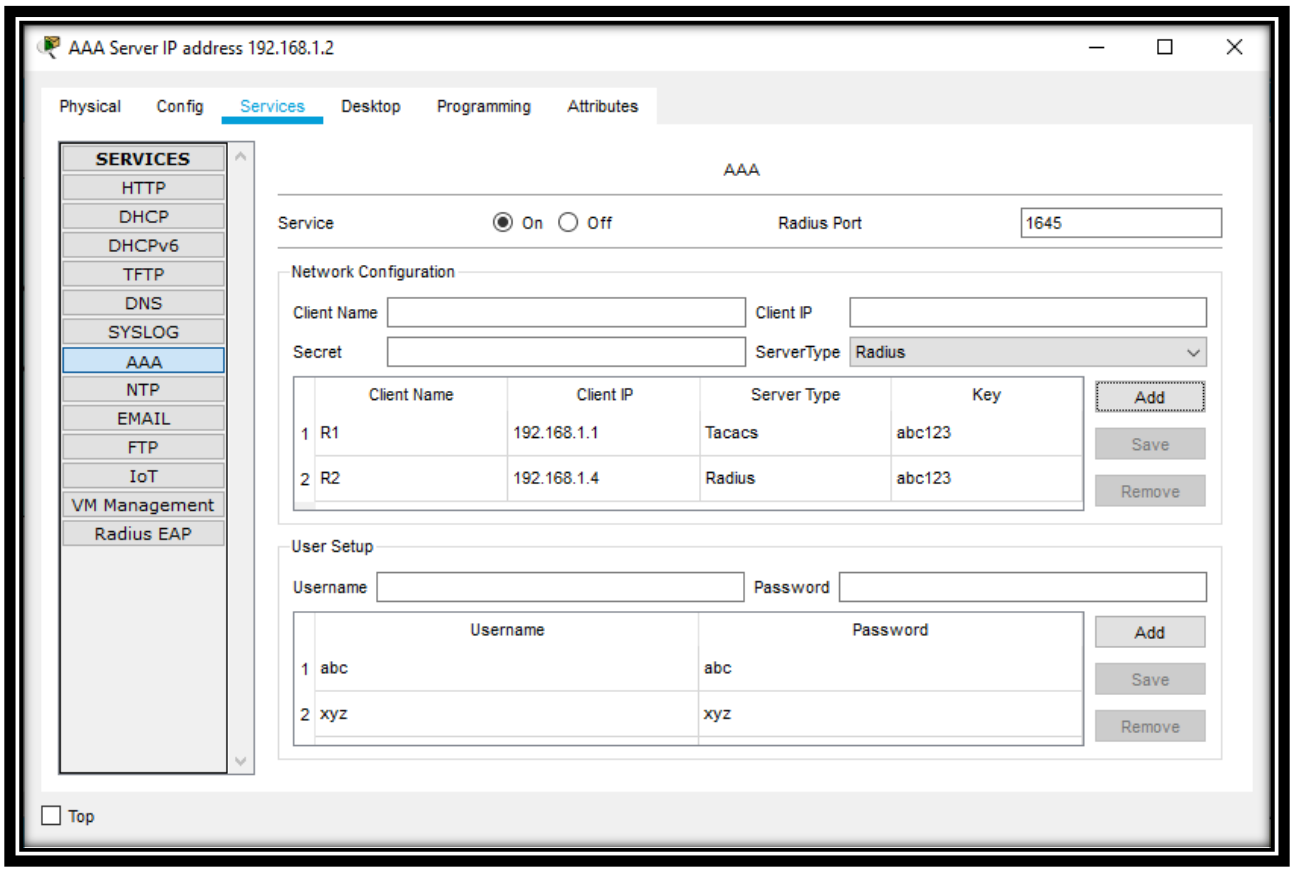
Network Access:

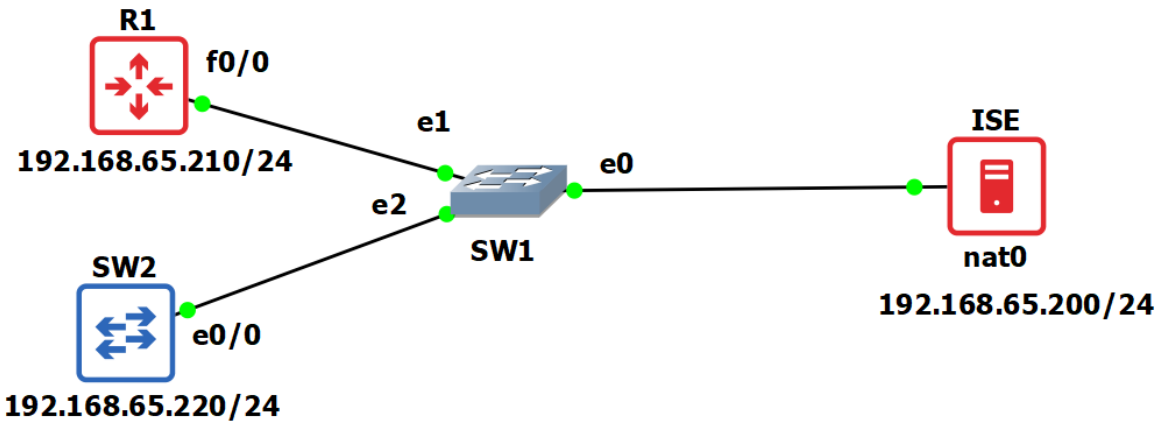
- Securing network access can provide the identity of the device or user.
- Secure network access is necessary in order to identify the user or endpoint.
- Before permitting the entity to communicate or access the network.
- AAA has important role in Network Access authentication and authorization.
- To filter legitimate user AAA Network access authentication is required.
- AAA authenticates these devices & control what these users are authorized for.
- There are two uses of AAA, Device Administration and Network Access.



R1 Configuration	R2 Configuration
en config t hostname R1 int f0/0 ip add 192.168.1.1 255.255.255.0 no sh aaa new-model Tacacs-server host 192.168.1.2 key abc123 aaa authentication login AAA group tacacs+ Line vty 0 1 login authentication AAA	en config t hostname R2 int f0/0 ip add 192.168.1.4 255.255.255.0 no sh aaa new-model radius-server host 192.168.1.2 key abc123 aaa authentication login AAA group radius Line vty 0 1 login authentication AAA

AAA Server Setting:





AAA with ISE Lab:

R1 Configuration:	SW1 Configuration:
en config t hostname R1 int f0/0 ip add 192.168.65.210 255.255.255.0 no sh !R1 AAA Configuration exit aaa new-model tacacs-server host 192.168.65.200 key test123 aaa authentication login default group tacacs+ local aaa authentication enable default group tacacs+ enable aaa authorization exec default group tacacs+ local aaa authorization commands 0 default group tacacs+ local aaa authorization commands 1 default group	en config t hostname SW1 int vlan 1 ip add 192.168.65.220 255.255.255.0 no sh !SW1 AAA Configuration exit aaa new-model tacacs server ISE address ipv4 192.168.65.200 key test123 aaa authentication login default group tacacs+ local aaa authentication enable default group tacacs+ enable aaa authorization exec default group tacacs+ local aaa authorization commands 0 default group tacacs+ local

tacacs+ local aaa authorization commands 15 default group tacacs+ local aaa authorization config-commands line vty 0 4 authorization commands 0 default authorization commands 1 default authorization commands 15 default authorization exec default login authentication default	aaa authorization commands 1 default group tacacs+ local aaa authorization commands 15 default group tacacs+ local aaa authorization config-commands line vty 0 4 authorization commands 0 default authorization commands 1 default authorization commands 15 default authorization exec default login authentication default

Troubleshoot Device Security Using IOS AAA:

- AAA debug commands are very useful in detecting the problems related with AAA.
- The Cisco IOS debug command output provides a valuable source of information.
- Another command line tool which is useful in testing AAA authentication is CLI "test"
- The "test" command can be used to show the output and to test AAA authentications.

AAA Needs to be Enabled:

- AAA is disabled by default on Cisco routers and switches, to enable use aaa new-model.

Method List Defines Authentication Methods:

- When no method list exists, the vty lines use the local username and password database.

Method List Service is Incorrect:

- The method list service must match the service for which you are creating the list.

Devices able to Reach AAA Server:

- Use the test aaa command on the Cisco Router or Cisco Switch to verify connectivity.
- Use Telnet to reach authentication port number of AAA server to verify connectivity.

Correct Pre-Shared Key:

- Ensure that the router and the AAA server are configured with the same pre-shared key.

Correct Ports to be Configured:

- RADIUS uses ports 1812 or 1645 (Cisco default) for authentication in Network devices.
- RADIUS uses ports 1813 or 1646 (Cisco default) for accounting in Network devices.

Correct AAA Server IP:

- The AAA server group needs to have the correct AAA server IP addresses configured.
- Also, may be wrong IP address of client is configured on AAA server (Cisco ISE, ACS).

Some T-shoot Command:
R# debug aaa authentication
R# debug aaa protocol local
R# debug radius authentication
R# debug tacacs authentication
R# debug aaa authorization
R# debug aaa accounting
R# debug tacacs
R# debug radius